Общество с ограниченной ответственностью

«Нордголд Менеджмент»

УТВЕРЖДАЮ

Генеральный директор

_____Н.Г. Зеленский

«03» марта 2014 г.

Положение о порядке обработки и защиты персональных данных в ООО «Нордголд Менеджмент»

Москва

2014г.

СОДЕРЖАНИЕ.

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Наименование документа:	*Положение о порядке обработки и защите персональных данных в ООО «Нордголд Менеджмент»*
Номер документа:	
Версия	*Разработан впервые.*
Утверждено	*Приказом Генерального директора ООО «Нордголд Менеджмент» №_____ от _____*
Дата введения в действие	*«__» _____ 20__ г.*
Дата пересмотра	*«01» декабря 2015 г.*
Цель процесса	*Процесс, регулируемый настоящим Положением, направлен на выполнение ряда требований по защите персональных данных физических лиц, обрабатываемых в информационных системах Общества, а также на организацию и проведение ряда мероприятий, в число которых, в том числе входит:* • *получение письменного согласия субъектов персональных данных на обработку своих персональных данных;* • *обеспечение должного уровня защищенности персональных данных;* • *приведение ИСПДн в соответствие с нормативными требованиями.*
Владелец процесса, структурное подразделение	*Дирекция по обеспечению бизнеса, Дирекция по персоналу*
Структурные подразделения – участники процесса	*Все структурные подразделения ООО «Нордголд Менеджмент»*

ОБЩИЕ ПОЛОЖЕНИЯ

Назначение документа:

Настоящее Положение разработано в целях организации защиты персональных данных от разглашения и несанкционированного доступа, обеспечения защиты прав и свобод работников ООО «Нордголд Менеджмент» (далее – «Общество», «Оператор») и иных физических лиц при обработке их персональных данных. Настоящее Положение устанавливает основные требования к порядку обработки персональных данных работников Общества и иных физических лиц, а также к мероприятиям по обеспечению безопасности персональных данных при их обработке в подразделениях Общества.

Требования настоящего Положения распространяются на все структурные подразделения Общества, в которых осуществляется обработка персональных данных.

Цели процесса:

Процесс, регулируемый настоящим Положением, направлен на выполнение ряда требований по защите персональных данных физических лиц, обрабатываемых в информационных системах Общества, а также на организацию и проведение ряда мероприятий, в число которых, в том числе входит:

- получение письменного согласия субъектов персональных данных на обработку своих персональных данных;

- обеспечение должного уровня защищенности персональных данных;

- приведение ИСПДн в соответствие с нормативными требованиями.

Показатели эффективности процесса:

Процесс, регулируемый настоящим Положением, считается успешным, если:

- определён Перечень персональных данных, обрабатываемых в Обществе;

- назначен ответственный за организацию обработки персональных данных;

- изданы документы, определяющие политику Общества в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в части защиты персональных данных, устранение последствий таких нарушений;

- применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных;

- работники Общества, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Принятые термины и сокращения:

Общество, Оператор	ООО «Нордголд Менеджмент» как Оператор
Положение	Положение о порядке обработки и защиты персональных данных в ООО «Нордголд Менеджмент»

Распространение информации	действия, направленные на получение информации неопределенным кругом лиц или на передачу информации неопределенному кругу лиц; связанные с опубликованием информации в средствах массовой информации, в том числе в электронных, информационно-телекоммуникационных сетях общего пользования (включая сеть "Интернет"); связанные с распространением информации через электронные, информационно-телекоммуникационные сети общего пользования (включая сеть "Интернет")
Персональные данные (далее также ПД, ПДн)	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
Обработка персональных данных	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Блокирование персональных данных	временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Уничтожение персональных данных	действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
Обезличивание персональных данных	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

Информационная система персональных данных (далее ИСПДн)	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

1. Порядок обработки персональных данных.

1.1 Основные принципы и условия обработки персональных данных.

1.1.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ актуальной редакции. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

6) осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

7) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1.1.2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных:

1) Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев:

a) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

b) персональные данные сделаны общедоступными субъектом персональных данных;

c) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

d) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

e) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

2) Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

1.1.3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение Оператора). Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации. В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с законодательством Российской Федерации.

1.1.4. Лицо, осуществляющее обработку персональных данных по поручению Оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

1.1.5. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом.

1.1.6. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

1.1.7. Согласие субъекта персональных данных на обработку его персональных данных:

1) Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

2) Согласие на обработку персональных данных может быть отозвано

субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в п.1.1.1 (со 2 по 7 подпункты), п.1.1.2 (подпункт 1 (b-e)).

3) Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, возлагается на Оператора.

4) В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

a) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

b) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

c) наименование или фамилию, имя, отчество и адрес Оператора, получающего согласие субъекта персональных данных;

d) цель обработки персональных данных;

e) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

f) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка будет поручена такому лицу;

g) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;

h) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

i) подпись субъекта персональных данных.

5) В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

6) В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

7) Персональные данные могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления Оператору подтверждения наличия оснований, указанных в п.1.1.7 подпункт 2.

1.1.8. Трансграничная передача персональных данных:

1) Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических

лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2) Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

a) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

b) исполнения договора, стороной которого является субъект персональных данных;

c) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

1.1.9. Действующее законодательство Российской Федерации предоставляет субъектам персональных данных следующие основные права:

1) Субъект персональных данных имеет право на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

2) Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных;

3) Субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

1.1.10. Оператор осуществляет следующие основные мероприятия по защите персональных данных:

1) разграничение доступа к персональным данным;

2) установление в отношении персональных данных режима конфиденциальности;

3) возложение на работников и контрагентов, получающих персональные данные, обязательства по обеспечению их конфиденциальности;

4) защита персональных данных в информационных системах посредством аппаратных и программных средств;

5) ограничение доступа к серверам и рабочим станциям, с помощью которых возможно получить доступ к информационным системам, содержащим персональные данные;

6) ограничение доступа в помещения, в которых персональные данные хранятся вне информационных систем (на бумажных и аналогичных носителях);

7) хранение персональных данных в любом формате исключительно в охраняемых помещениях с соблюдением противопожарных и иных технических норм.

1.1.11. Оператор может возлагать выполнение отдельных мероприятий по защите персональных данных, в т.ч. из числа указанных в п. 1.1.10 настоящего положения, на сторонние организации (подрядчиков, исполнителей).

1.1.12. Решения, порождающие юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы,

не могут приниматься Оператором на основании исключительно автоматизированной обработки персональных данных.

1.1.13. Оператор приказом генерального директора должен назначить соответствующее уполномоченное подразделение (уполномоченное лицо), ответственное за защиту персональных данных (далее - «Уполномоченное подразделение по защите», «Уполномоченное лицо»).

1.1.14. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных субъекта персональных данных должны соблюдать следующие общие требования:

1) при определении объема и содержания, обрабатываемых персональных данных Оператор должен руководствоваться Конституцией РФ, Трудовым кодексом РФ, Гражданским кодексом РФ и иными федеральными законами;

2) в той степени, в которой это требуется согласно действующему законодательству РФ и настоящему Положению, Оператор знакомит субъектов персональных данных и их представителей с документами Оператора, устанавливающими порядок обработки их персональных данных;

1.1.15. В процессе хранения персональных данных должны обеспечиваться:

1) соблюдение требований нормативных документов Оператора, устанавливающих правила хранения конфиденциальных сведений;

2) сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством РФ и настоящим Положением;

3) контроль достоверности и полноты персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

1.1.16. Оператор использует в процессе обработки персональных данных следующие способы обработки персональных данных:

1) автоматизированную обработку персональных данных;

2) обработку персональных данных без использования средств автоматизации.

1.2 Доступ к персональным данным

1.2.1. Обязательными условиями доступа к персональным данным, обрабатываемым Обществом, за исключением общедоступных персональных данных, как для его работников, так и для его контрагентов, являются:

1) принятие обязательства по обеспечению конфиденциальности персональных данных;

2) ознакомление под роспись с Перечнем обрабатываемых Обществом персональных данных и с настоящим Положением, а также принятие обязательства по его соблюдению.

1.2.2. Неограниченный доступ ко всем персональным данным, обрабатываемым Обществом, предоставляется генеральному директору Общества. Генеральный директор Общества вправе своими приказами определить работников Общества, уполномоченных на предоставление допуска к персональным данным (далее – «Лица со специальными полномочиями») с указанием ПДн, к которым они вправе предоставлять допуск.

1.2.3. Лица, указанные в п. 1.2.2. настоящего положения, вправе предоставлять доступ к персональным данным, обрабатываемым Обществом, путем выдачи допуска, в котором указывается:

- фамилия, имя, отчество, должность лица, которому предоставлен допуск,
- цель допуска;
- описание персональных данных, к которым предоставляется допуск;
- операции с персональными данными, которые разрешены допущенному лицу;

- срок действия допуска.

1.2.4. Лица со специальными полномочиями принимают решение о допуске работников кадровой службы, бухгалтерии, других подразделений Общества к персональным данным работников, контрагентов Общества и других субъектов обработки ПДн в объеме, необходимом для выполнения своих должностных обязанностей (как они определены в соответствующих должностных инструкциях) и организуют учет сотрудников, допущенных к ПДн.

1.2.5. Во избежание сомнений, соблюдение условий допуска к персональным данным, обрабатываемым Обществом (п.1.2.1 настоящего Положения), является обязательным для всех лиц, указанных в п.п. 1.2.2-1.2.4 настоящего Положения.

1.2.6. При переводе (увольнении) работника, имеющего доступ к обработке персональных данных, его учетная запись (права) должны быть заблокированы. Если по новому месту работы в Обществе этому работнику вновь требуется доступ к персональным данным, то процедура доступа повторяется.

1.2.7. Лица со специальными полномочиями в объеме своих полномочий должны ежегодно организовывать проведение сверки по ролям и работникам, обрабатывающим персональные данные. Цель проверки – минимизация полномочий, а также выявление и блокирование учетных записей пользователей, которым доступ к обработке персональных данных не требуется.

1.3 Перечень персональных данных, обрабатываемых Обществом. Реестр информационных систем персональных данных и архивов персональных данных.

1.3.1. Перечень персональных данных, обрабатываемых Обществом (далее – «Перечень»), ведется Директором по персоналу.

1.3.2. В Перечне указываются персональные данные граждан, чьи данные обрабатываются в Обществе по категориям, и видам персональных данных.

1.3.3. По каждому виду персональных данных указывается:

- содержание персональных данных;
- категория данных;
- источник получения;
- основание для обработки;

1.3.4. Непосредственно персональные данные в Перечень не включаются.

1.3.5. Запрещается изменение Перечня без согласования с Директором по персоналу.

1.3.6. Уполномоченное подразделение по защите (Уполномоченное лицо) ведет Реестр информационных систем персональных данных, в котором содержится информация обо всех имеющихся в Обществе информационных системах ПДн (далее – ИСПДн), представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

1.3.7. Дополнительно в Реестр записывается информация об архивах персональных данных (далее - «АПД»), т.е. совокупности персональных данных, представленных не в электронном виде и хранящихся вне информационных систем, на бумажном или ином носителе, объединенных на основе критерия места хранения и цели обработки (бухгалтерия, дирекция по персоналу и т.п.).

1.3.8. В отношении каждой ИСПДн/каждого АПД в Реестре указывается:

1) наименование ИСПДн/АПД;
2) место нахождения ИСПДн/АПД (адрес, помещение);
3) общая характеристика субъектов, персональные данные которых хранятся в

ИСПДн/АПД (контрагенты, работники, их отдельные категории и т.д.);

4) общая характеристика персональных данных, хранящихся в ИСПДн/АПД (реквизиты договоров, бухгалтерская информация, кадровая документация и т.д.);

5) результат классификации ИСПДн/АПД;

6) подразделение, в интересах которого осуществляется ведение ИСПДн/ АПД (далее - «Заинтересованное подразделение»);

7) лицо, ответственное за работу с ИСПДн/АПД (назначается приказом Генерального директора Общества).

8) наличие/отсутствие в ИСПДн/АПД специальных категорий персональных данных (п. 1.1.9. настоящего положения).

1.3.9. Непосредственно персональные данные в Реестр не включаются.

1.3.10. Лица, ответственные за работу с ИСПДн и АПД, обязаны незамедлительно информировать Уполномоченное подразделение по защите (Уполномоченное лицо) о любых известных изменениях, подлежащих отражению в Реестре. Уполномоченное подразделение по защите (Уполномоченное лицо) на регулярной основе запрашивает у указанных выше лиц информацию о текущих характеристиках ИСПДн и АПД, необходимых для ведения Реестра.

1.3.11. Реестр ведется в электронном виде.

1.4 Обработка запросов субъектов персональных данных.

1.4.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Оператором способы обработки персональных данных;

4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании ФЗ;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные ФЗ.

11) уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.4.2. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям:

1) В случае, если сведения, указанные в п.1.4.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту

персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п.1.4.1, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен ФЗ, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

2) Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п.1.4.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса;

3) Отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

1.4.3. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

1.4.4. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Оператор обязан дать в письменной форме мотивированный ответ, с указанием основания для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

1.4.5. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

1.4.6. Запросы субъектов ПДн по п. 1.4.1. (далее – «Запросы») направляются получившим их подразделением в Уполномоченное подразделение по защите (Уполномоченному лицу) не позднее следующего рабочего дня после их получения.

Сотрудник Уполномоченного подразделения по защите (Уполномоченное лицо) производит учет Запроса и в течение одного рабочего дня проверяет соответствие Запроса требованиям действующего законодательства РФ (п.3 ст. 14 ФЗ-152 «О персональных

данных»). Если Запрос не соответствует требованиям действующего законодательства РФ, сотрудник Уполномоченного подразделения по защите (Уполномоченное лицо) готовит мотивированный письменный ответ за своей подписью и отправляет его лицу, направившему Запрос.

Если поступивший Запрос соответствует требованиям действующего законодательства РФ и касается получения сведений о наличии у Оператора его персональных данных, ознакомления с такими персональными данными, то в целях подготовки ответа сотрудник Уполномоченного подразделения по защите (Уполномоченное лицо):

- направляет в кадровую службу Запрос субъекта ПДн;
- выявляет список ИСПДн/АПД в которых содержаться ПДн субъекта поступившего Запроса и направляет внутренние запросы лицам, ответственным за работу с этими ИСПДн/АПД .

Ответственные за работу с ИСПДн/АПД в срок не более трех рабочих дней направляют ответы на указанные внутренние запросы в кадровую службу Общества.

1.4.4. На основании информации, полученной в соответствии с п. 1.4.3 настоящего положения, работник кадровой службы готовит ответ на Запрос, который должен быть подписан от имени Общества работником кадровой службы, обладающим необходимыми полномочиями, и направлен заявителю (субъекту ПДн).

1.4.5. При ознакомлении субъекта Запроса с соответствующими ПДн (Запрос поступил от работника Общества), а равно при корректировке ПДн на основании устного запроса субъекта ПДн, факт ознакомления с ПДн/корректировки ПДн должен свидетельствоваться распиской субъекта запроса.

1.4.6. Если Запрос субъекта ПДн соответствует требованиям действующего законодательства РФ и касается корректировки своих ПДн (в том случае, когда ПДн являются неполными, устаревшими или недостоверными: изменения паспортных данных, состава семьи и т.п.), то такие Запросы сотрудник Уполномоченного подразделения по защите (Уполномоченное лицо) сразу перенаправляет на исполнение в кадровую службу Общества.

1.4.7. Работник кадровой службы информирует работника Уполномоченного подразделения по защите (Уполномоченное лицо) относительно ответов на Запросы субъектов ПДн (дата и номер исходящего документа) и хранит в кадровой службе в течение 5 лет Запросы, ответы на них и иные доказательства направления таких ответов. При наличии в Запросе или у Общества почтового адреса лица, направившего Запрос, сотрудник кадровой службы обязан, наряду с другими способами коммуникаций, направить ответ на Запрос заказным письмом и хранить доказательства такого направления. При возможности выдать ответ на Запрос под расписку (например – работникам Общества), ответ на Запрос выдается под расписку, подлежащую хранению сотрудником кадровой службы.

1.4.8. При обращении работников Общества (их законных представителей) с устными требованиями: об ознакомлении с кадровой документацией (личными делами и иными стандартизированными документами кадрового учета установленной формы), о получении копий такой документации, о получении справок с места работы, а равно при предоставлении работниками Общества документов и информации, направленной на корректировку их ПДн в целях кадрового учета, ознакомление работников со своими персональными данными, выдача соответствующих справок и корректировка ПДн осуществляется в порядке, установленном Директором по персоналу, в срок, не превышающий трех рабочих дней с момента соответствующего обращения. При этом производится идентификация личности обратившегося субъекта (его законного представителя) на основании удостоверяющих личность документов. При устном обращении законного представителя субъекта персональных данных также производится проверка его полномочий. Такие запросы в Уполномоченном подразделении

(Уполномоченным лицом) учету не подлежат.

1.4.9. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

1.4.10. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

1.4.11. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

1.4.12. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п. 1.4.11 – п.1.4.11, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

1.4.13. Запросы субъектов персональных данных, касающиеся:

- получение сведений об Операторе, о месте его нахождения;

- уточнения, блокирования или уничтожения ПДн субъекта ПДн, направившего Запрос, в случае, если его ПДн являются, незаконно полученными, не являются необходимыми для заявленной цели обработки или в случае их неправомерного использования

направляются сотрудником Уполномоченного подразделения по защите (Уполномоченным лицом) в Дирекцию по персоналу Общества не позднее следующего рабочего дня после их получения.

Дополнительно сотрудник Уполномоченного подразделения (Уполномоченное лицо) предоставляет сотруднику Дирекции по персоналу информацию по ИСПДн/АПД, где могут находится ПДн субъекта требующие уточнения, блокирования или уничтожения.

1.4.14. Сотрудник Дирекции по персоналу, осуществлявший обработку Запроса, информирует сотрудника Уполномоченного подразделения по защите (Уполномоченное лицо) относительно ответов на Запросы субъектов ПДн (дата и номер исх. документа). Запросы, ответы на них и доказательства направления таких ответов хранятся в Дирекции по персоналу в течение 5 лет. При наличии в Запросе или у Общества почтового адреса лица, направившего Запрос, сотрудник Дирекции по персоналу обязан, наряду с другими способами коммуникаций, направить ответ на Запрос заказным письмом и хранить доказательства такого направления. При возможности выдать ответ на Запрос под расписку (например – работникам Общества), ответ на Запрос выдается под расписку, подлежащую хранению сотрудником Дирекции по персоналу.

2. Защита персональных данных в ИСПДн.

2.1 Меры, направленные на обеспечение выполнения Оператором обязанностей

2.1.1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных нормативными правовыми актами РФ. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей. К таким мерам могут, в частности, относиться:

1) назначение Оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание Оператором, являющимся юридическим лицом, документов, определяющих политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных нормативным правовым актам РФ, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей;

6) ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2.1.2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

2.1.3. Оператор обязан представить документы и локальные акты, и (или) иным образом подтвердить принятие мер, по запросу уполномоченного органа по защите прав субъектов персональных данных.

2.2 Меры по обеспечению безопасности персональных данных при их обработке.

2.2.1. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.2.2. Правительство РФ с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

2.2.3. Состав и содержание необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

2.2.4. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.3 Требования к защите персональных данных при их обработке в информационных системах персональных данных

2.3.1. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

2.3.2. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Разделяют угрозы следующих типов:

1) угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

2) угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

3) угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

2.3.3. Типы информационных систем:

1) Информационная система является информационной системой, обрабатывающей специальные категории персональных данных (далее ИСПДн-С), если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

2) Информационная система является информационной системой, обрабатывающей биометрические персональные данные (далее ИСПДн-Б), если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

3) Информационная система является информационной системой, обрабатывающей общедоступные персональные данные (далее ИСПДн-О), если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных;

4) Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в (1) - (3) пункта 2.3.3.

5) Информационная система является информационной системой, обрабатывающей персональные данные сотрудников Оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных

случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками Оператора.

2.3.4. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных:

1) Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

a) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

b) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора.

2) Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

a) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

b) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора;

c) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

d) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора;

e) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора;

f) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора.

3) Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

a) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников Оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора;

b) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных

данных сотрудников Оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора;

c) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора;

d) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

e) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора.

4) Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

a) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

b) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками Оператора.

2.3.5. Сводная таблица соответствия типов ИСПДн типам актуальных угроз

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4

2.3.6. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

1) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

2) обеспечение сохранности носителей персональных данных;

3) утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

4) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

2.3.7. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных п. 2.3.5 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

2.3.8. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных п. 2.3.6 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

2.3.9. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных п. 2.3.7 настоящего документа, необходимо выполнение следующих требований:

1) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника Оператора по доступу к персональным данным, содержащимся в информационной системе;

2) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

2.3.10. Контроль за выполнением настоящих требований организуется и проводится Оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые Оператором (уполномоченным лицом).

2.4 Действия в случае обнаружения нарушения правил использования ИСПДн

2.4.1. Лицо, обнаружившее факт нарушения правил использования ИСПДн (несанкционированные доступ, изменение ИСПДн, несоблюдение условий хранения персональных данных и т.п.), обязано сообщить об этом своему непосредственному руководителю и в Уполномоченное подразделение по защите (Уполномоченному лицу).

2.4.2. По факту обращения, указанного в п. 2.3.1, руководитель Уполномоченного подразделения по защите (Уполномоченное лицо) инициирует проверку, для проведения которой могут привлекаться любые необходимые специалисты Общества.

2.4.3. Проверка должна быть проведена и закончена в течение 10 рабочих дней с момента обнаружения факта нарушения правил пользования ИСПДн.

2.4.4. Срок, предусмотренный п. 2.4.3 настоящего положения, может быть продлен руководителем Уполномоченного подразделения (Уполномоченным лицом), но не более чем на 20 рабочих дней.

2.4.5. Результаты проверки должны быть оформлены в виде заключения, содержащего:

1) описание выявленных фактов нарушения правил пользования ИСПДн;

2) выводы о причинах и условиях, приведших к допущенным нарушениям;

3) предложения о дальнейших действиях, связанных с выявленными нарушениями (инициирование юридических процедур, направленных на привлечение виновных лиц к ответственности и взыскании с них сумм причиненного ущерба, принятие мер по минимизации негативных последствий нарушения для субъектов персональных данных и Общества и т.п.);

4) предложения по устранению причин и условий, приведших к допущенным нарушениям (совершенствование ИСПДн, изменение режима доступа к ней, пересмотр результатов классификации ИСПДн и т.п.).

2.4.6. Результаты проверки должны быть доведены до сведения лица, ответственного за работу с ИСПДн не позднее одного рабочего дня с момента их оформления. Доведение результатов проверки до сведения лица, обнаружившего факт нарушения правил пользования ИСПДн, осуществляется исключительно по требованию такого лица и при условии, что при этом не разглашаются конфиденциальные сведения, доступ к которым у такого лица отсутствует.

3. Особенности обработки и защиты персональных данных в АПД.

3.1. Основные способы защиты персональных данных в АПД.

3.1.1. Лица, осуществляющие обработку персональных данных в АПД, наряду с соблюдением условий, установленных п. 1.2 настоящего Положения, должны быть проинформированы об особенностях и правилах такой обработки, установленных Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждены Постановлением Правительства РФ от 15 сентября 2008 г. № 687) (далее – «Правила»), иными нормативными актами Российской Федерации и настоящим Положением.

3.1.2. Все АПД, имеющие различные цели обработки, должны храниться отдельно.

3.1.3. Доступ в помещения, в которых хранятся АПД, предоставляется исключительно лицам, имеющим допуск к соответствующим АПД (их частям). Указанные помещения должны находиться исключительно в охраняемых зданиях (с контрольно-пропускным режимом), запираться, при этом факт доступа в них должен, по возможности, фиксироваться (электронные системы, журналы выдачи ключей и т.п.).

3.1.4. Материальные носители, входящие в состав АПД и содержащие персональные данные, должны соответствовать п.п. 4,5,7,8, 9 и 11 Правил.

3.2. Хранение материальных носителей, содержащих персональные данные в составе АПД.

3.2.1. В целях обеспечения сохранности персональных данных в составе АПД и исключения несанкционированного доступа к ним Обществом приняты следующие меры:

1) ограничение и контроль доступа в помещения, в которых хранятся АПД (раздел 1.2, п. 3.1.3 настоящего положения);

2) осуществление обработки персональных данных в АПД способами, исключающими доступ к ним не уполномоченных лиц, в том числе посредством дистанционного наблюдения (запрет на вынос материальных носителей, содержащих персональные данные из мест их хранения, использование жалюзи на окнах, иные необходимые меры);

3) поддержание помещений, в которых хранятся АПД, в технически пригодном состоянии, в т.ч. в строгом соответствии с противопожарными нормами и правилами;

4) запрет на пронос любой электронной и фото-видеоаппаратуры в помещения, используемые для хранения АПД;

5) недопустимость перевода документов АПД в электронный формат, за исключением случаев использования в составе ИСПДн в соответствии с настоящим положением;

6) возложение на работников Общества обязанности по соблюдению настоящего положения, Правил и иных нормативных актов Российской Федерации при обработке персональных данных в составе АПД, привлечение их к дисциплинарной ответственности за нарушение данной обязанности.

3.2.2. Меры, перечисленные в п. 3.2.1 настоящего положения, реализуются безусловно, непрерывно и в отношении всех имеющихся в распоряжении Общества АПД.

3.2.3. Ответственность за реализацию мер, предусмотренных п. 3.2.1 настоящего Положения, в отношении каждого конкретного АПД возлагается на лицо, ответственное за работу с ним (назначается приказом Генерального директора Общества) и указанное в этом качестве в Реестре.

3.3. Действия в случае обнаружения нарушения правил использования АПД.

3.3.1. Лицо, обнаружившее факт нарушения правил использования АПД (несанкционированный доступ, несоблюдение мер, перечисленных в п. 3.2.1 настоящего положения и т.п.), обязано сообщить об этом своему непосредственному руководителю и в Уполномоченное подразделение по защите (Уполномоченному лицу).

3.3.2. По факту обращения, указанного в п. 3.3.1, руководитель Уполномоченного подразделения по защите (Уполномоченное лицо) инициирует проверку, для проведения которой могут привлекаться любые необходимые специалисты Общества.

3.3.3. Проверка должна быть проведена и закончена в течение 10 рабочих дней с момента обнаружения факта нарушения правил пользования АПД.

3.3.4. Срок, предусмотренный п. 3.3.3 настоящего положения, может быть продлен руководителем Уполномоченного подразделения по защите (Уполномоченным лицом), но не более чем на 20 рабочих дней.

3.3.5. Результаты проверки должны быть оформлены в виде заключения, содержащего:

1) описание выявленных фактов нарушения правил пользования АПД;

2) выводы о причинах и условиях, приведших к допущенным нарушениям;

3) предложения о дальнейших действиях, связанных с выявленными нарушениями (инициирование юридических процедур, направленных на привлечение виновных лиц к ответственности и взыскании с них сумм причиненного ущерба, принятие мер по минимизации негативных последствий нарушения для субъектов персональных данных и Общества и т.п.);

4) предложения по устранению причин и условий, приведших к допущенным нарушениям (совершенствование АПД, изменение режима доступа к нему и т.п.).

3.3.6. Результаты проверки должны быть доведены до сведения лица, ответственного за работу с АПД не позднее одного рабочего дня с момента их оформления. Доведение результатов проверки до сведения лица, обнаружившего факт нарушения правил пользования АПД, осуществляется исключительно по требованию такого лица и при условии, что при этом не разглашаются конфиденциальные сведения, доступ к которым у такого лица отсутствует.

4. Обязанности, Ответственность и Контроль

4.1 Обязанность лиц со специальными полномочиями:

4.1.1. Рассмотрение и принятие решений (совместно с Уполномоченным подразделением по защите (Уполномоченным лицом) относительно:

- мест хранения и осуществления конфиденциального делопроизводства в отношении ПДн;
- новых ИС, в которые требуется передать ПДн из существующих ИСПДн;
- сбор новых ПДн в существующие ИСПДн.

4.1.2. В системе разрешения доступа к обработке ПДн:

- принятие решений о доступе к обработке ПДн (только по ИСПДн Общества, в которые осуществляется ввод конфиденциальных ПДн);
- организация учета лиц, получивших доступ к обработке ПДн в ИСПДн;
- организация сверки по ролям в ИСПДн.

4.2 Обязанность Уполномоченного подразделения по защите (Уполномоченного лица):

- осуществление внутреннего контроля за соблюдением Оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников Оператора положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организацию, прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов в Обществе.

4.3 Обязанность участников процедуры ответов на запросы субъектов ПДн:

4.3.1. Уполномоченное подразделение по защите (Уполномоченное лицо):

- первичная экспертиза запросов;
- учет поступивших запросов и ответов на них;
- контроль сроков исполнения процедуры ответов на запросы субъектов ПДН участниками процедуры;
- проведение расследований по фактам нарушений режима защиты ПДн.

4.3.2. Кадровая служба

- своевременное исполнение процедуры формирования ответов на запросы субъектов ПДн в части ее касающейся;
- учет и хранение запросов и ответов на запросы, обработанных Дирекцией по персоналу.
- своевременное исполнение процедуры формирования ответов на запросы субъектов ПДн в части, ее касающейся;
- учет и хранение запросов и ответов на запросы в случаях, предусмотренных настоящим Положением.

4.3.3. Ответственные за работу с ИСПДн/АПД :

- достоверность и точность предоставляемой информации по запрашиваемому субъекту ПДн;
- проверка факта недостоверности персональных данных в установленные настоящим Положение сроки;
- блокирование (разблокирование), уничтожение ПДн субъекта ПДн по решению уполномоченного сотрудника (юриста) в установленные настоящим Положением сроки;
- учет лиц, получивших доступ к обработке ПДн в ИСПДн;
- ежегодная сверка по ролям и пользователям, обрабатывающим персональные данные.

4.4 Ответственность за неисполнение или ненадлежащее исполнение:

Неисполнение или ненадлежащее исполнение требований и условий настоящего Положения работниками, ответственными за его исполнение в силу должностных обязанностей, влечет за собой применение к ним мер дисциплинарного или иного воздействия, предусмотренных правилами внутреннего трудового распорядка, нормативными документами об оплате труда и о премировании и другими внутренними документами Общества.

4.5 Условия и порядок пересмотра и контроля

4.5.1. Плановая проверка актуальности Положения производится ежегодно с целью определения необходимости его пересмотра для обеспечения соответствия реальным условиям и актуальным требованиям к обеспечению безопасности персональных данных обрабатываемых в Обществе. Плановая проверка актуальности Положения проводится Уполномоченным подразделением по защите (Уполномоченным лицом) В результате проверки устанавливается возможность продления или необходимость пересмотра действующей редакции Положения.

4.5.2. Внеочередной пересмотр Положения производится по решению Уполномоченного подразделения по защите (Уполномоченного лица) в случае выявления неадекватности определенного Положения комплекса мероприятий законодательству и нормативно-правовым актам, регулирующим обработку персональных данных.

4.5.3. Пересмотр Положения осуществляет Уполномоченное подразделение по защите (Уполномоченное лицо), которое готовит предложения по частичной переработке документа (выпуск редакции с изменениями), либо полной переработке документа (перевыпуск в новой редакции).